THE CITY OF REDWOOD CITY INVITES APPLICATIONS FOR:

SUPERVISING I.T. ANALYST (INFORMATION SECURITY PROGRAM MANAGER)

WORKING TITLE

#25A-58

ANNUAL SALARY:
$171,392 - $205,649 + Excellent Benefits

Opened July 28, 2025, with first review of applications August 11, 2025. Opened until filled.

Interested in joining the Redwood City team?

Application Process
Apply online, click here:
https://www.calopps.org/redwood-city/job-20646758

Apply: Immediately, with first review of application 8/11/25

City application is required in CalOpps. Candidates with a disability, which may require special assistance in any phase of the application or selection process, should advise the Human Resources Division upon submittal of application.

Selection Process: Oral Board Interviews to schedule the end of August

All applications, including supplemental questionnaire, will be reviewed for neatness, accuracy, completion, relevant education, experience, training and other job-related qualifications. Those who best meet the stated qualifications and requirements for the position will be invited to participate in the testing process, which will consist of an oral board interview.

WHY JOIN THE REDWOOD CITY TEAM?

We offer a wide range of meaningful career opportunities with potential for growth, training and development, competitive salaries, flexible work schedules, paid time off, and robust benefits. The Redwood City team is guided by the core values of ***excellence, integrity, service, collaboration, inclusion and innovation***. Inherent in these values is a great organizational culture based on trust, strong and supportive leadership, respect, risk-taking, empowerment, and effective communication.

The community is known for its inclusivity, strong engaged neighborhoods, and civic pride. The City works diligently to maintain positive and productive relationships with community partners, together providing outstanding services, programs and opportunities for residents and businesses. This mix of tradition and progress, community, and diversity, makes Redwood City an extraordinary place to work and call home.

ABOUT THE POSITION

The City of Redwood City is seeking an experienced and forward-thinking cybersecurity professional to serve as its Information Security Program Manager (working title), classified as a Supervising Information Technology Analyst. This newly created leadership role will oversee the planning, coordination, and execution of the City's cybersecurity program across all departments, vendors, systems, and platforms.

Reporting to the IT Director, the Information Security Program Manager will lead the development and delivery of Redwood City's multi-year cybersecurity roadmap. The role will direct implementation of security tools, standards, and controls in alignment with frameworks such as NIST CSF, Cal-Secure, and Executive Order 14028. This position will also manage the City's Cybersecurity Annual Training Program, including accountability mechanisms for enforcement, and serve as the internal authority on cybersecurity policy, infrastructure, and vendor compliance.

The Program Manager will direct and supervise the day-to-day work performed by internal staff and consultants — including activities such as risk assessments, penetration testing, vulnerability mitigation, and compliance reporting. They will lead the implementation of cybersecurity policies and procedures, oversee incident response and post-event analysis, and ensure the security posture of third-party vendors and cloud environments meets City standards.

This role also maintains operational partnerships with external cybersecurity and regulatory agencies including CalOES, CJIS, MS-ISAC, and DHS, coordinating assessments, training, and intelligence-sharing to ensure continuity and compliance. The Program Manager will provide senior-level guidance to City leadership while empowering the IT cybersecurity team to deliver the technical and procedural protections required to safeguard City assets.

BENEFITS

The successful candidate will enjoy the following benefits in RCMEA MOU

- **Public Employees Retirement System**: *(PERS)*. New members join 2% at age 62; current members join 2% at age 60.
- **Health Insurance:** The City pays 90% of premium, up to $2,461/Mo. In 2025
- **Dental Insurance:** City paid 90% premium.
- **Vision Insurance:** City paid 90% premium.
- **Life Insurance**
- **Long Term Disability**
- **Employee Assistance Program**
- **Vacation leave**: l0-25 days per year
- **Sick leave:** 12 days per year
- **Paid holidays**:15 days per year
- **Bereavement Leave:** Up to 3 days/yr.
- **Fitness center:** access at City facilities
- **Education** Reimbursement program: $2,000 per year.
- **Deferred Compensation** Plan (457). The city contributes 2% of your salary to a deferred compensation plan.
- **Commuter program** available City matches up to $100/month on commuter expenses.

Core Values:

To serve and enhance Redwood City's community, our employees strive to carry out a set of Core Purpose and Values

This position offers a rare opportunity to establish Redwood City's first centralized cybersecurity program and lead a dedicated team in building the City's long-term security strategy — grounded in public trust, operational readiness, and digital resilience.

THE IDEAL CANDIDATE

The ideal candidate is a cybersecurity leader with a proven track record in building and managing enterprise-wide security programs. They bring strong technical expertise, deep familiarity with compliance frameworks (such as NIST CSF, Cal-Secure, HIPAA, and CJIS), and the ability to assess and mitigate risk across complex, public-sector environments.

They are a strategic thinker and a clear communicator, able to translate cybersecurity risks into actionable direction for City leadership, departments, and vendors. The ideal candidate excels at leading teams, coordinating interdepartmental initiatives, and enforcing policy through structured implementation and accountability.

Experience in cybersecurity policy development, supervising implementation of training and response programs, and evaluating third-party security posture is essential. A collaborative, service-oriented mindset and a commitment to advancing digital trust and public safety will drive success in this role.

MINIMUM QUALIFICATIONS

Any combination of experience and training that would likely provide the required knowledge and abilities are qualifying. A typical way to obtain the knowledge and abilities would be:

Training & Education

Education: Bachelor's degree in cybersecurity, computer science, information technology, or a related field. A master's degree is desirable.

Certifications (Preferred): Relevant certifications such as CISSP, CISM, GSEC, CRISC, or CompTIA Security+ are strongly preferred.

Experience

The ideal candidate will have at least five (5) years of progressively responsible experience in cybersecurity or IT infrastructure, including two (2) years in a supervisory or lead capacity. *(This experience should demonstrate the candidate's ability to oversee security programs, direct incident response efforts, assess organizational risk, and apply regulatory frameworks such as NIST CSF, Cal-Secure, HIPAA, or CJIS.)*

Familiarity with evaluating vendor risk, cloud security, and third-party platforms is essential. Prior experience leading cross-functional security initiatives and supervising staff or consultants in a public-sector environment is highly desirable.

Licenses

Valid California Driver's License or the ability to obtain within three months.

Knowledge of:

- Cybersecurity frameworks and regulations, including NIST CSF, Cal-Secure, CJIS, and HIPAA
- Penetration testing, vulnerability management, and risk assessment practices
- Incident response, threat detection, and mitigation strategies
- Cloud security principles and third-party/vendor risk evaluation
- Development and enforcement of security policies, procedures, and training programs
- Supervisory practices for managing technical staff and external cybersecurity resources

Ability to:

- Develop, implement, and lead citywide cybersecurity strategies and initiatives
- Assess risks, oversee penetration testing, and manage incident response and recovery
- Collaborate with vendors and third parties to ensure ongoing compliance and up-to-date security practices
- Interpret and apply laws, regulations, and standards such as NIST CSF, Cal-Secure, CJIS, and HIPAA
- Communicate technical information clearly to both executive leadership and technical teams
- Supervise, coach, and evaluate technical staff and manage external security resources
- Operate various desktop and host computer equipment.

To review the job description please click: www.redwoodcity.org/home/showpublisheddocument/564/635779290627400000

Prior to Appointment

Candidates will be required to pass a pre-employment physical exam and extensive background check *(at no cost to the candidate)* including the following:

- Criminal History Check
- DMV Check
- DOJ fingerprint check
- Reference check. Reference checks will be conducted in close coordination with the candidate.

SPECIAL INSTRUCTIONS

A City application and supplemental questionnaire is required. Applications must be filled out completely. Failure to list work experience, and education or training or stating "See Resume" in the work experience section of the application will be considered an incomplete application. Resumes may be attached separately, but resumes will not be accepted in lieu of a city application.

SUPPLEMENTAL QUESTIONNAIRE

The supplemental questionnaire is a key component of your application and will be used to assist us in evaluating your qualifications, background, analytical ability and writing skills.

Limit each response to 300–500 words. While we limit the number of words per question, we encourage you to take your time to reflect on the prompts and submit thoughtful, complete, and nuanced answers. We anticipate that candidates should easily be able to answer all questions without going beyond the recommended 300 - 500 words per question.

1. Describe a cybersecurity program or initiative you led that involved multiple departments or stakeholders. What was your role, what framework or methodology did you apply (e.g., NIST CSF, Cal-Secure), and what were the outcomes?

2. Provide an example of a significant cybersecurity incident you handled or coordinated. What actions did you take, who was involved, and what lessons were applied afterward?

3. Redwood City relies on vendors and cloud providers for essential services. Describe how you have evaluated or enforced security compliance with third-party partners. What processes or tools did you use?

4. Share your experience developing, implementing, or enforcing cybersecurity policies and employee training programs. How did you drive adoption and ensure accountability across the organization?

5. What role have you played in conducting or overseeing cybersecurity risk assessments or penetration testing? How did you use the findings to improve your organization's security posture?